

FILED

AO-106 (Rev. 06/09)-Application for Search Warrant

UNITED STATES DISTRICT COURT

JUL 25 2024

for the
Northern District of Oklahoma

Heidi D. Campbell, Clerk
U.S. DISTRICT COURT

In the Matter of the Search of)
An Apple iPhone with a Lock Screen Depicting Jeffry)
Clain, and an Apple iPhone with a Blue Lock Screen,)
Currently Stored at Homeland Security Investigations –)
Tulsa at 125 West 15th Street, Suite 500, Tulsa, Oklahoma)
74119)

Case No.

24-mj-498-SH

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 2422(b)

Attempted Coercion and Enticement of a Minor


18 U.S.C. §§ 2252(a)(4)(B) and
(b)(2)

Possession of and Access with Intent to View Child Pornography

The application is based on these facts:

See Affidavit of SA Dustin Carder, HSI, attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: ____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Dustin Carder, Special Agent, HSI
Printed name and title

Subscribed and sworn to by phone.

Date:

7/25/24


Judge's signature

City and state: Tulsa, Oklahoma

Susan E. Huntsman, U.S. Magistrate Judge
Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of
An Apple iPhone with a Lock Screen
Depicting Jeffry Clain, and an Apple
iPhone with a Blue Lock Screen,
Currently Stored at Homeland Security
Investigations – Tulsa at 125 West 15th
Street, Suite 500, Tulsa, Oklahoma
74119**

Case No. _____

FILED UNDER SEAL

**Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize**

I, Dustin L. Carder, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I have been employed as a Special Agent ("SA") with Homeland Security Investigations ("HSI") since December 2018. I am currently assigned to the Office of

the Resident Agent in Charge in Tulsa, Oklahoma, and am currently assigned to investigate crimes involving child exploitation. While employed by HSI, I have investigated federal criminal violations related to child exploitation and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center's ("FLETC") twelve-week Criminal Investigator Training Program ("CITP") and the sixteen-week Homeland Security Investigations Special Agent Training ("HSISAT") program, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have received focused child exploitation training covering topics such as: undercover chatting concepts and techniques, interview techniques, live streaming investigations, undercover investigations, capturing digital evidence, transnational child sex offenders, correlations between child pornography and hands-on offenses, psychological and behavioral characteristics of sex offenders, and mobile messaging platforms utilized by these types of offenders. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2422.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events

and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. § 2422(b) – (Attempted Coercion and Enticement of a Minor), and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) – (Possession of and Access with Intent to View Child Pornography) will be located in the electronically stored information described in Attachment B and is recorded on the device described in Attachment A.

Jurisdiction

6. “[A] warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States.” 18 U.S.C. § 3103a.

7. The requested search is related to the following violations of federal law:

a. Title 18, United States Code, Section 2422(b) which states that whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life.

b. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) which state that any person who knowingly possesses, or knowingly

accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if — (i)the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii)such visual depiction is of such conduct shall be punished as provided in subsection (b) of this section.

8. Venue is proper because the property described in this affidavit is located within the Northern District of Oklahoma. Fed. R. Crim. P. 41(b)(1).

Identification of the Device to be Examined

9. The property to be searched consists of **an Apple iPhone with a lock screen depicting Jeffry CLAIN, and an Apple iPhone with a blue lock screen**, pictured in Attachment A, hereinafter the “Devices.” The Devices are currently located at Homeland Security Investigations – Tulsa at 125 West 15th Street, Suite 500, Tulsa, Oklahoma 74119, within the Northern District of Oklahoma.

10. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

Technical Terms

11. The following definitions apply to this Affidavit and Attachment B:

a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Cloud-based storage service,” as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

c. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

d. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); any device that can be used to connect to the Internet including a router and a modem; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also

encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

g. “Hashtag,” as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

h. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

i. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

j. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

k. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

l. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

n. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

o. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether stored in a permanent format.

Background on Child Pornography, Computers, the Internet and Email

12. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

- a. Computers and digital technology have dramatically changed the way in which individuals interested in children interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
- b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store in excess of 300 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to

a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP's) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small

devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Media storage devices can easily be concealed and carried on an individual’s person. Smartphones and/or mobile phones are also often carried on an individual’s person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing

this information can be intentional (i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

h. A device known as a router in conjunction with a modem allows numerous computers to connect the Internet and other computers through the use of telephone, cable, or wireless connection. A router, in conjunction with a modem, can connect literally millions of computers around the world. Routers often store information as to which computer used a modem to connect to the Internet at a specific time and location. This information when viewed along with the traces or "footprints" can provide valuable information on who distributed and/or received a visual depiction of a minor engaged in sexually explicit conduct and who possessed and accessed with intent to view a visual depiction of a minor engaged in sexually explicit conduct.

Specifics of Search and Seizure of Computer Systems

13. Based upon my training and experience, and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;
- b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer

hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort

through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

14. Based on my experience and my consultation with other agents and officers who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU).

Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

15. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to

access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

Probable Cause

16. In July 2024, Special Agents from Homeland Security Investigations along with several members of the Tornado Alley Child Exploitation and Trafficking Taskforce (TACETT) conducted an undercover chat operation in Tulsa, Oklahoma, in the Northern District of Oklahoma.

17. On July 19, 2024, Tulsa Police Detective Raymond Ackermann was online conducting undercover investigations personifying as a 14-year-old male child. Ackermann created an account on an online application¹ utilizing an age-regressed photograph of himself. Without any solicitation, a subject who identified himself as “Jeff” reached out to Det. Ackermann and said, “You’re handsome,” and “Are you interested in being friends with an older gentleman?” Det. Ackermann informed “Jeff” that he was 14, to which “Jeff” responded, “nice.”

18. Communications between “Jeff” and Det. Ackermann continued throughout July 19, 2024, and July 23, 2024. During that timeframe, “Jeff” sent the following messages to Det. Ackermann after it had been clearly established that Det. Ackermann was personifying a 14-year-old male child (the following are excerpts and not the verbatim or entirety of the conversations):

¹ The identity of online application is being withheld from this affidavit to protect the integrity of ongoing and future undercover operations.

- a. “What grade are you in ?” (Suspect)
- b. “Im goigin to 9th” (Ackermann)
- c. “I want to come over too lol” (Suspect)
- d. “I’m horny and nervous now lol” (Suspect)
- e. “It’s been years since I’ve dated a young guy like you” (Suspect)
- f. “I really want to at least meet you in person somewhere” (Suspect)
- g. “Did you want my massage to lead to something else ?” (Suspect)
- h. “If your nude I’d probably give you a hand job till you cum” (Suspect)
- i. “Maybe finger your ass” (Suspect)
- j. “You can always come by after school when I’m home” (Suspect)
- k. “What colors your building” – (Suspect)
- l. “Yellow” – (Ackermann)
- m. “Are you here?” – (Ackermann)
- n. “Yes” – (Suspect)
- o. “Apartment208” – (Ackermann)
- p. “Come get me please” – (Suspect)

19. On July 23, 2024, “Jeff” wanted to meet the 14-year-old male child at the child’s residence. Det. Ackermann provided “Jeff” with the address of an undercover residence in the City of Tulsa, within the Northern District of Oklahoma. During the conversations, “Jeff” stated that he drives a Honda vehicle.

20. On July 23, 2024, at approximately 1510 hours, Special Agents and Officers observed a grey Honda Accord bearing Oklahoma EJN707 enter the parking

lot of the undercover location. A white male subject exited the vehicle and sat on the curb outside. The male subject appeared visually similar to the visible features in a photograph that the subject sent to Det. Ackermann.

21. At approximately 1515 hours, Special Agents and Officers took the white male subject into custody. The male subject was identified as Jeffry Alan CLAIN (DOB XX/XX/1966). While taking CLAIN into custody, Special Agents and Officers observed CLAIN had two phones, **an Apple iPhone with a lock screen depicting Jeffry CLAIN, and an Apple iPhone with a blue lock screen**, the Devices, on his person. At the time of the arrest, one of the phones was unlocked and open to communications with the undercover officer. The chats read:

- a. “What colors your building” – (Suspect)
- b. “Yellow” – (Ackermann)
- c. “Are you here?” – (Ackermann)
- d. “Yes” – (Suspect)
- e. “Apartment208” – (Ackermann)
- f. “Come get me please” – (Suspect)

22. After his arrest, CLAIN was interviewed, and post-Miranda, made multiple statements of interest:

- a. That the profile photograph [of the undercover] was of an obvious minor.
- b. That he wanted to give a “hand job” and “finger” the minor.
- c. That he knew it was illegal to have sexual relations with someone under the age of 16.

- d. That he has previously engaged in sexual intercourse with a 14-year-old male subject while he was an adult.
- e. That there is child pornography on his phone.

23. CLAIN was arrested for violation of 18 U.S.C. § 2422(b) – (Attempted Coercion and Enticement of a Minor).

24. I know from training and experience that individuals who exhibit a sexual interest in children and/or attempt to coerce or entice a minor often have multiple victims. This will often include sexually explicit media files of minor victims and/or minors engaged in sexually explicit conduct. For these reasons, I believe that evidence of the offenses listed herein will be located on the Devices.

25. The Devices are currently in the lawful possession of HSI. They came into HSI's possession in the following way: incident to arrest of CLAIN. Therefore, while HSI might already have all necessary authority to examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

26. The Devices are currently in storage at Homeland Security Investigations – Tulsa at 125 West 15th Street, Suite 500, Tulsa, Oklahoma 74119. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of HSI.

Electronic Storage and Forensic Analysis

27. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

28. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of

information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer

behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to coerce or entice minor victims, transfer obscene material to minors, receive/distribute child pornography, and possess child pornography, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire

medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

28. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

29. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the Devices. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications.

Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

30. Based on the information above, I submit that there is probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

31. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Respectfully submitted,



Dustin L. Carder
Special Agent
Homeland Security Investigations

Subscribed and sworn to by phone on July 25, 2024.



SUSAN E. HUNTSMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

The property to be searched are **an Apple iPhone with a lock screen depicting Jeffry CLAIN, and an Apple iPhone with a blue lock screen**, hereinafter the “Devices.” The Devices are currently located at Homeland Security Investigations – Tulsa at 125 West 15th Street, Suite 500, Tulsa, Oklahoma 74119, within the Northern District of Oklahoma. The Devices to be searched are described above and pictured below.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.



ATTACHMENT B

Particular Things to be Seized

All records on the Device(s) described in Attachment A that relate to 18 U.S.C. § 2422(b) – (Attempted Enticement of a Minor to Engage in Sexual Activity), and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) – (Possession of and Access with Intent to View Child Pornography) involving Jeffry CLAIN, including:

1. Information, correspondence, records, documents, or other materials pertaining to the enticement or coercion of minors to engage in sexual acts or sexual conduct, as defined in 18 U.S.C. 2422(b), that were transmitted or received using the cellular device or computer;
2. Images and videos of child pornography; files containing images and data of any type relating to the sexual exploitation of minors, and material related to the possession or production thereof;
3. Information, correspondence, records, documents, or other materials pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C 2256, or pertaining to the sexual exploitation of minors, that were transmitted or received using the cellular device;
4. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;

5. Records relating to communication with others as to the criminal offenses listed above; including incoming and outgoing voice messages; text messages; emails; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Facebook, Snapchat, and other applications that can assign roaming phone numbers; and other Internet-based communication media;
6. Records relating to documentation or memorialization of the criminal offenses listed above, including voice memos, photographs, videos, and other audio and video media, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos, including device information, geotagging information, and information about the creation date of the audio and video media;
7. Records relating to the planning and execution of the criminal offenses above, including Internet activity, firewall logs, caches, browser history, and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;
8. Application data relating to the criminal offenses above; and
9. All records and information related to the geolocation of the Devices.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.